PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312261
(43)Date of publication of application : 25.10.2002

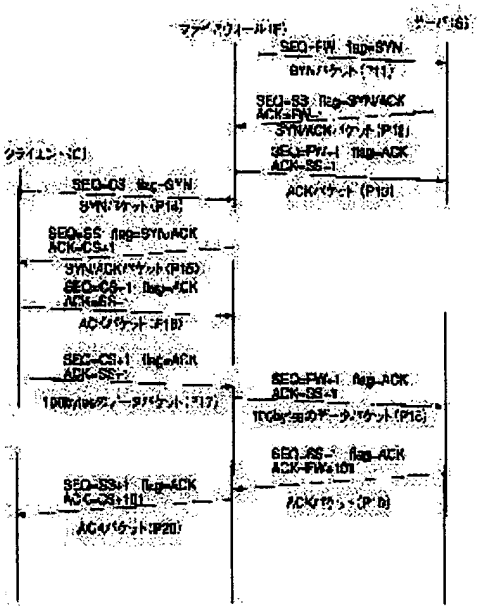
(51)Int.Cl. G06F 13/00
H04L 12/66

(21)Application number : 2001-110528
(22)Date of filing : 09.04.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KAJIWARA FUMIO
OKABE KEIICHI
MORIAI SATOSHI

(54) NETWORK SERVICE RELAY METHOD AND RELAY DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To construct a firewall having both performance deciding up to justice of a service request similarly to an 'application gateway' and shortness of a response time equivalent to 'packed filtering'.
SOLUTION: In the fire wall (F), connection between the firewall (F) and a server (S) is previously established to the server (S) and is managed. Thereby, a connection load to the server (S) when a client (C) requests connection is reduced, and speed-up relay processing is realized by only rewriting an SEQ number and an ACK number when relaying TCP data packets between the server (S) and the client (C). The firewall (F) has a function of verifying the justice in the case of service request transfer, and cuts off injustice request transfer.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号　✓
特開2002－312261
（P2002－312261A）
(43)公開日　平成14年10月25日(2002.10.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｃ	５Ｂ０８９
	３５１		３５１Ｚ	５Ｋ０３０
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	

審査請求　未請求　請求項の数18　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－110528(P2001－110528)

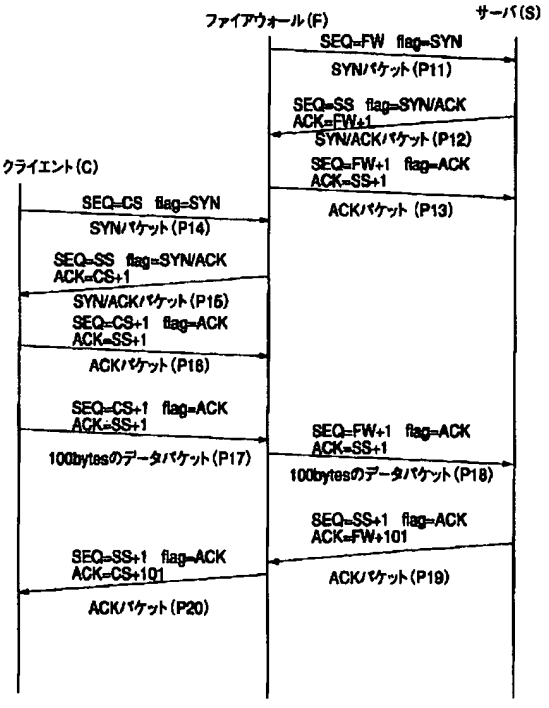
(22)出願日　平成13年４月９日(2001.4.9)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　梶原　史雄
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　岡部　恵一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100058479
弁理士　鈴江　武彦　（外２名）

最終頁に続く

(54)【発明の名称】　ネットワークサービス中継方法及び中継装置

(57)【要約】
【課題】　「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築する。
【解決手段】　ファイアウォール（Ｆ）において、予めサーバ（Ｓ）との間でファイアウォール－サーバ間コネクションを確立し、管理しておくことで、クライエント（Ｃ）からのコネクション要求時のサーバ（Ｓ）への接続負荷を軽減し、サーバ（Ｓ）とクライエント（Ｃ）との間のＴＣＰデータパケット中継時にはＳＥＱ番号およびＡＣＫ番号の書き換えのみとすることで、中継処理の高速化を実現する。さらにサービス要求転送時に正当性を検証する機能を持たせ、不正な要求転送を遮断する。



1

【特許請求の範囲】

【請求項１】　任意の二つのコンピュータ間でのコネクションを双方のコネクションキーに基づいて確立可能なネットワークに適用され、あるコンピュータ上のサーバによって提供されるサービスを、そのコンピュータとは別のコンピュータ、もしくは同一のコンピュータによって提供されるファイアウォールを介して、他のコンピュータ上のクライエントに提供するネットワークサービス中継方法であって、

前記ファイアウォールと前記サーバとの間に予め１本以上のファイアウォールーサーバ間コネクションを確立し、前記コネクションに用いられた前記サーバ側と前記ファイアウォール側のコネクションキーを保持しておく第１のステップと、

前記クライエントと前記ファイアウォールとの間に第１のステップで保持しておいた前記サーバ側コネクションキーの一つを用いてクライエントーファイアウォール間コネクションを確立し、前記コネクションの確立に用いられた前記クライエント側のコネクションキーと前記ファイアウォール側のコネクションキーを保持する第２のステップと、

前記クライエントーファイアウォール間コネクションと前記ファイアウォールーサーバ間コネクションとを結合・中継する第３のステップとを具備することを特徴とするネットワークサービス中継方法。

【請求項２】　前記第３のステップは、前記クライエントから届くメッセージのコネクションキーを前記ファイアウォールーサーバ間コネクションの前記ファイアウォール側のコネクションキーに書き換えて前記サーバへ転送し、前記サーバから届くメッセージのコネクションキーを前記クライエントーファイアウォール間コネクションの前記クライエント側のコネクションキーに書き換えて前記クライエント側へ転送することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項３】　前記第１のステップは、予め管理収容本数として整数Ｍ（Ｍ≧１）が指定されているとき、前記クライエントーファイアウォール間コネクションと未結合のファイアウォールーサーバ間コネクションと、クライエントーファイアウォール間コネクションと結合済みのファイアウォールーサーバ間コネクションを合わせた、ファイアウォールーサーバ間コネクションの合計がＭ本以下となるように、ファイアウォールーサーバ間コネクションの確立を制限することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項４】　前記第１のステップは、予め初期の管理収容本数として整数Ｎ（Ｍ≧Ｎ≧１）が指定されているとき、初期状態でＮ本の未結合ファイアウォールーサーバ間コネクションを確立する初期化処理を実行することを特徴とする請求項３に記載のネットワークサービス中継方法。

2

【請求項５】　前記第１のステップは、前記ファイアウォールーサーバ間コネクションの合計がＭ本以下のとき、前記未結合ファイアウォールーサーバ間コネクションの切断または前記クライエントーファイアウォール間コネクションとの結合により前記未結合ファイアウォールーサーバ間コネクションがＮ本より少なくなった場合に、新たに未結合ファイアウォールーサーバ間コネクションを確立して、Ｎ本の未結合ファイアウォールーサーバ間コネクションを維持することを特徴とする請求項４に記載のネットワークサービス中継方法。

【請求項６】　前記第２のステップは、前記ファイアウォールーサーバ間コネクションと結合していない未結合のクライエントーファイアウォール間コネクションと、前記ファイアウォールーサーバ間コネクションと結合済みのファイアウォールークライエント間コネクションとを合わせた、クライエントーファイアウォール間コネクションの合計が、前記第１のステップで確立されている前記ファイアウォールーサーバ間コネクションの合計を上回らないように、クライエントーファイアウォール間コネクションの確立を制限することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項７】　前記第２のステップは、新たにクライエントからファイアウォールに対してコネクション確立要求があった場合に、前記未結合ファイアウォールーサーバ間コネクションの数と前記未結合クライエントーファイアウォール間コネクションの数を比較し、

サーバ側コネクション数よりクライエント側コネクション数が上回っていれば、新たにクライエントーファイアウォール間コネクションを確立し、

クライエント側コネクション数がサーバ側コネクション数と同数か下回るようであれば、クライエントからのコネクション確立要求を廃棄するか、あるいは、前記未結合ファイアウォールーサーバ間コネクションの数が前記未結合クライエントーファイアウォール間コネクションの数を上回るまでクライエントーファイアウォール間コネクション確立を遅延することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項８】　前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記クライエントーファイアウォール間コネクションを通じて前記クライエントからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、

不正と判定された場合に、当該クライエントーファイアウォール間コネクションを切断し、

不正なしと判定された場合に、未結合のファイアウォールーサーバ間コネクションと結合し、当該メッセージを当該ファイアウォールーサーバ間コネクションを通じて前記サーバへ転送することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項９】　前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記クライエントーファイアウォール間コネクションを通じて前記クライエントからの追加のメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、
不正と判定された場合に、当該クライエントーファイアウォール間コネクション及び当該クライエントーファイアウォール間コネクションと結合済みのファイアウォールーサーバ間コネクションを切断し、
不正なしと判定された場合に、受信した追加のメッセージを当該クライエントーファイアウォール間コネクションと結合しているファイアウォールーサーバ間コネクションを通じて前記サーバへ転送し、
不正ではないが、追加のメッセージでないと判定された場合に、受信したメッセージを当該クライエントーファイアウォール間コネクションと結合しているファイアウォールーサーバ間コネクションを通じてそのままサーバへ転送することを特徴とする請求項８に記載のネットワークサービス中継方法。

【請求項１０】　前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記ファイアウォールーサーバ間コネクションを通じて前記サーバからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、
不正と判定された場合に、当該ファイアウォールーサーバ間コネクション及び当該ファイアウォールーサーバ間コネクションと結合済みのクライエントーファイアウォール間コネクションを切断し、
不正なしと判定された場合に、当該ファイアウォールーサーバ間コネクションと結合しているクライエントーファイアウォール間コネクションを通じて前記クライエントへメッセージを転送し、
不正ではないがメッセージでないと判定された場合に、当該ファイアウォールーサーバ間コネクションと結合しているクライエントーファイアウォール間コネクションを通じてそのまま前記クライエントへ転送することを特徴とする請求項１に記載のネットワークサービス中継方法。

【請求項１１】　前記管理収容本数を、前記サーバからの制御信号により指定・変更することを特徴とする請求項３、４、５のいずれかに記載のネットワークサービス中継方法。

【請求項１２】　前記管理収容本数を、一つ以上のクライエントをまとめた複数のクライエントグループが存在するとき、クライエントグループごとに指定・変更することを特徴とする請求項３、４、５のいずれかに記載のネットワークサービス中継方法。

【請求項１３】　前記管理収容本数を、一つ以上のサーバをまとめた複数のサーバグループが存在するとき、サーバグループごとに指定・変更することを特徴とする請求項３、４、５のいずれかに記載のネットワークサービス中継方法。

【請求項１４】　サーバ・クライエントサービスが行われるネットワークシステムに適用され、サーバコンピュータとクライエントコンピュータとの間で伝送される情報を中継し、ファイアウォールとして機能するネットワークサービス中継装置であって、
前記サーバコンピュータとの間で予め決められた本数で、クライエントーファイアウォール間コネクションと未結合のファイアウォールーサーバ間コネクションを確立し管理する未結合コネクション管理手段と、
前記クライエントコンピュータのうち新規にコネクション要求のあったクライエントコンピュータとの間でクライエントーファイアウォール間コネクションを確立する新規コネクション処理手段と、
前記新規コネクション処理手段で確立されたクライエントーファイアウォール間コネクションにより結合されたクライエントコンピュータからのサービス要求について正当性を検証するサービス要求正当性検証手段と、
前記サービス要求正当性検証手段で正当性が認められたとき、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとを結合して被検証サービス要求をサーバコンピュータに転送し、正当性が認められないとき、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合を切断するコネクション間中継処理手段とを具備することを特徴とするネットワークサービス中継装置。

【請求項１５】　さらに、前記コネクション間中継処理手段でクライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合によりサーバコンピュータから送出されるサービス応答について正当性を検証するサービス応答検証手段を備え、
前記コネクション中継処理手段は、前記サービス応答検証手段で正当性が認められたとき、被検証サービス要求をクライエントコンピュータに転送し、正当性が認められないとき、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合を切断することを特徴とする請求項１４にネットワークサービス中継装置。

【請求項１６】　前記未結合コネクション管理手段は、ファイアウォールーサーバ間コネクションの最大収容本数が指定されているとき、クライエントーファイアウォール間コネクションと未結合のファイアウォールーサーバ間コネクション数を最大収容本数以内に制限することを特徴とする請求項１４に記載のネットワークサービス中継装置。

【請求項１７】　前記ネットワークシステムがＴＣＰ／

ＩＰ（Transport Communication Protocol／Internet Protocol）で構築されているとき、
前記コネクション間中継処理手段は、ＴＣＰ層とＩＰ層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はＴＣＰ層に配置され、前記サービス要求正当性検証手段はアプリケーション層に配置されることを特徴とする請求項１４に記載のネットワークサービス中継装置。

【請求項１８】　前記ネットワークシステムがＴＣＰ／ＩＰ（Transport Communication Protocol／Internet Protocol）で構築されているとき、
前記コネクション間中継処理手段は、ＴＣＰ層とＩＰ層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はＴＣＰ層に配置され、前記サービス要求正当性検証手段及びサービス応答正当性検証手段はアプリケーション層に配置されることを特徴とする請求項１４に記載のネットワークサービス中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、任意の二つのコンピュータ間で確立可能なネットワークにおいて、あるコンピュータによって提供されるサービスを、ファイアウォールを介して他のコンピュータに提供するネットワークサービス中継方法及び中継装置に関する。

【０００２】

【従来の技術】コンピュータネットワーク上の２つのコンピュータ間でコネクションを確立するためのネットワークプロトコルの標準として、ＴＣＰ（Transport Communication Protocol：伝送制御プロトコル）＜ＲＦＣ７６１参照＞がある。ＴＣＰでは、「３ウェイ・ハンドシェイク」という方法でコネクションを確立する。図６にその様子を示す。

【０００３】ここで、ＴＣＰパケットのヘッダには、データパケットでデータの番号を表すＳＥＱ（シーケンス）番号、正常に受け取ったデータの次のデータを要求するＡＣＫ（確認応答）番号、ＳＹＮ（同期）フラグ、ＡＣＫフラグなどが含まれており、ＴＣＰコネクションの確立に使われる。

【０００４】ＴＣＰでコネクションを確立する際には、まず、クライエント（Ｃ）からサーバ（Ｓ）に対してＳＹＮパケット（Ｐ１）を送る。ＳＹＮパケット（Ｐ１）にはクライエントが無作為に決定した初期ＳＥＱ番号「ＣＳ」が含まれており、同時にＳＹＮフラグを有効とすることで、コネクションの確立を要求していることを表している。

【０００５】サーバ（Ｓ）は、クライエント（Ｃ）からのＳＹＮパケット（Ｐ１）が到着すると、そのクライエント（Ｃ）に対してＳＹＮパケット（Ｐ１）を受け取ったことを伝えるために、ＳＹＮ／ＡＣＫパケット（Ｐ２）を生成してクライエント（Ｃ）へ送る。このＳＹＮ／ＡＣＫパケット（Ｐ２）の生成では、クライエント（Ｃ）からのＳＥＱ番号に１を加えた値「ＣＳ＋１」をＡＣＫ番号に設定し、ＡＣＫフラグを有効にすると同時に、サーバ（Ｓ）自身が無作為に決定した初期ＳＥＱ番号「ＳＳ」を設定してＳＹＮフラグを有効にしている。

【０００６】クライエント（Ｃ）では、サーバ（Ｓ）からＳＹＮ／ＡＣＫパケット（Ｐ２）を受け取った時点でコネクションが確立する。但し、サーバ（Ｓ）側ではまだコネクションが確立していないので、クライエント（Ｃ）はＡＣＫパケット（Ｐ３）を生成してサーバ（Ｓ）に送る。このＡＣＫパケット（Ｐ３）の生成では、ＳＥＱ番号にサーバ（Ｓ）から送られてきたＳＹＮ／ＡＣＫパケット（Ｐ２）のＡＣＫ番号に示された番号「ＣＳ＋１」を設定し、ＡＣＫ番号にＳＹＮ／ＡＣＫパケット（Ｐ２）のＳＥＱ番号に１を加えた値「ＳＳ＋１」を設定している。

【０００７】サーバ（Ｓ）側にこのＡＣＫパケット（Ｐ３）が到着した時点で、クライエント（Ｃ）とサーバ（Ｓ）両側のＳＥＱ番号が同期され、サーバ（Ｓ）側でもコネクションが確立する。コネクション確立後はクライエント（Ｃ）、サーバ（Ｓ）のいずれの側からでもデータを送ることができる。

【０００８】例えば、クライエント（Ｃ）からサーバ（Ｓ）へ最初のデータを送る際には、ＳＥＱ番号には「ＣＳ＋１」を設定し、ＡＣＫ番号には「ＳＳ＋１」を設定して、ＡＣＫフラグを有効にしたデータパケット（Ｐ４）を送る。さらに、追加のデータを送る際には、先程送った１００bytesのデータの次を表すＳＥＱ番号「ＣＳ＋１０１」、ＡＣＫ番号には「ＳＳ＋１」を設定してＡＣＫフラグを有効にしたデータパケット（Ｐ５）を送る。

【０００９】データを受け取ったサーバ（Ｓ）はクライエント（Ｃ）に対して適当なタイミングでＡＣＫパケット（Ｐ６）を送る。この際のＡＣＫパケット（Ｐ６）を送る場合には、ＡＣＫ番号にその時点で受信済みのデータ（ＳＥＱ番号でＣＳ＋２５０）の次のＳＥＱ番号を表す「ＣＳ＋２５１」を設定し、ＳＥＱ番号に「ＳＳ＋１」を設定し、ＡＣＫフラグを有効にする。

【００１０】コンピュータネットワークでは、ネットワークを通じてサービスを提供するサーバとサービスを受けるクライエントがある。ＨＴＴＰ（ハイパーテキスト転送プロトコル）＜ＲＦＣ１９４５参照＞に基づくＷＷＷ（World Wide Web）サーバとＷＷＷブラウザ、ＦＴＰ（ファイル転送プロトコル）＜ＲＦＣ９５９参照＞に基づくＦＴＰサーバとＦＴＰクライエントなどはその好例である。

【００１１】ところで、上記のようなサービスをネットワーク上で提供するサーバとして動作させているサーバコンピュータは、侵入やサービス拒否攻撃（Denial of

Service Attack）などの攻撃を受けることが多い。このような攻撃からサーバコンピュータを守る手段として、ファイアウォールをサーバコンピュータの手前に設置する方法がある。

【００１２】このファイアウォールでサーバコンピュータを守る手法には、大きくわけて「パケット・フィルタリング」と「アプリケーション・ゲートウェイ」の二種類がある。

【００１３】前者の「パケット・フィルタリング」は、ネットワークを通じて通信を行う単位であるパケットをチェックすることでサーバを守るようにした手法である。すなわち、パケットには宛先となるコンピュータのＩＰアドレスとサービス種別を表すポート番号が含まれていることに着目し、特定のＩＰアドレスとポート番号の組み合わせを持つパケットのみを通すようにした手法である。例えば、ＩＰアドレスが（１０．０．０．１）のサーバコンピュータでWWWサービスを提供したい場合は、サーバコンピュータのＩＰアドレスである（１０．０．０．１）とWWWサービスのポート番号である（８０）を持つパケットだけを通すように設定する。

【００１４】後者の「アプリケーション・ゲートウェイ」は、ファイアウォールがクライエントからのサービス要求などのメッセージを全て受け取って、サービスのルールに従っているかどうかを判断し、ルールに従っている場合は、同じ内容のサービス要求を作ってサーバコンピュータへ転送し、当該サーバコンピュータからの返答をクライエントへ中継するという手法である。

【００１５】

【発明が解決しようとする課題】しかしながら、従来のファイアウォールの「パケット・フィルタリング」による手法では、パケットをチェックするだけなので、アプリケーションレベルのサービス要求が不正であったりする場合はこれをチェックすることができない。例えば、WWWサーバへのサービス拒否攻撃を行う場合はWWWクライエントからのWWWサービス要求の形をとる場合が多いが、このような攻撃は「パケット・フィルタリング」では防ぐことができない。また、大量のコネクション確立要求をサーバに要求するという方式のサービス拒否攻撃も「パケット・フィルタリング」では防げない。

【００１６】他方の「アプリケーション・ゲートウェイ」による手法であれば、クライエントのサービス要求がサービスのルールに従っているかどうかを判断するので、上記の例のようなサービス拒否攻撃を防ぐことができる。しかしながら、「アプリケーション・ゲートウェイ」はサーバとクライエントの間にたって互いの間の通信を中継する形となり、通常はＯＳ（Operating System）の上のアプリケーションとして実現されているので、前者の「パケット・フィルタリング」と比べると、クライエントがサービス要求を送信してからサーバからの返答を受信するまでの応答時間が長くなってしまう。

【００１７】本発明は、上記の問題を解決するためになされたもので、その目的とするところは、「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築したネットワークサービス中継方法及び中継装置を提供することにある。

【００１８】また、本発明の他の目的は、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバの代わりにクライエントとの間にコネクションを確立することができ、これによって新規コネクション確立にかかるサーバの負担を軽減することにある。

【００１９】また、本発明の他の目的は、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバとクライエントとの間のコネクションの数を管理することができ、これによってサービス提供にかかるサーバの負荷を管理することにある。

【００２０】

【課題を解決するための手段】上記の目的を達成するために本発明に係るネットワークサービス中継方法は、以下のような特徴的構成を備える。

【００２１】（１）任意の二つのコンピュータ間でのコネクションを双方のコネクションキーに基づいて確立可能なネットワークに適用され、あるコンピュータ上のサーバによって提供されるサービスを、そのコンピュータとは別のコンピュータ、もしくは同一のコンピュータによって提供されるファイアウォールを介して、他のコンピュータ上のクライエントに提供するネットワークサービス中継方法であって、前記ファイアウォールと前記サーバとの間に予め１本以上のファイアウォールーサーバ間コネクションを確立し、前記コネクションに用いられた前記サーバ側と前記ファイアウォール側のコネクションキーを保持しておく第１のステップと、前記クライエントと前記ファイアウォールとの間に第１のステップで保持しておいた前記サーバ側コネクションキーの一つを用いてクライエントーファイアウォール間コネクションを確立し、前記コネクションの確立に用いられた前記クライエント側のコネクションキーと前記ファイアウォール側のコネクションキーを保持する第２のステップと、前記クライエントーファイアウォール間コネクションと前記ファイアウォールーサーバ間コネクションとを結合・中継する第３のステップとを具備することを特徴とする。

【００２２】（２）（１）の構成において、前記第３のステップは、前記クライエントから届くメッセージのコネクションキーを前記ファイアウォールーサーバ間コネクションの前記ファイアウォール側のコネクションキーに書き換えて前記サーバへ転送し、前記サーバから届くメッセージのコネクションキーを前記クライエントーフ

ァイアウォール間コネクションの前記クライエント側のコネクションキーに書き換えて前記クライエント側へ転送することを特徴とする。

【００２３】（３）（１）の構成において、前記第１のステップは、予め管理収容本数として整数Ｍ（Ｍ≧１）が指定されているとき、前記クライエントーファイアウォール間コネクションと未結合のファイアウォールーサーバ間コネクションと、クライエントーファイアウォール間コネクションと結合済みのファイアウォールーサーバ間コネクションを合わせた、ファイアウォールーサーバ間コネクションの合計がＭ本以下となるように、ファイアウォールーサーバ間コネクションの確立を制限することを特徴とする。

【００２４】（４）（３）の構成において、前記第１のステップは、予め初期の管理収容本数として整数Ｎ（Ｍ≧Ｎ≧１）が指定されているとき、初期状態でＮ本の未結合ファイアウォールーサーバ間コネクションを確立する初期化処理を実行することを特徴とする。

【００２５】（５）（４）の構成において、前記第１のステップは、前記ファイアウォールーサーバ間コネクションの合計がＭ本以下のとき、前記未結合ファイアウォールーサーバ間コネクションの切断または前記クライエントーファイアウォール間コネクションとの結合により前記未結合ファイアウォールーサーバ間コネクションがＮ本より少なくなった場合に、新たに未結合ファイアウォールーサーバ間コネクションを確立して、Ｎ本の未結合ファイアウォールーサーバ間コネクションを維持することを特徴とする。

【００２６】（６）（１）の構成において、前記第２のステップは、前記ファイアウォールーサーバ間コネクションと結合していない未結合のクライエントーファイアウォール間コネクションと、前記ファイアウォールーサーバ間コネクションと結合済みのファイアウォールークライエント間コネクションとを合わせた、クライエントーファイアウォール間コネクションの合計が、前記第１のステップで確立されている前記ファイアウォールーサーバ間コネクションの合計を上回らないように、クライエントーファイアウォール間コネクションの確立を制限することを特徴とする。

【００２７】（７）（１）の構成において、前記第２のステップは、新たにクライエントからファイアウォールに対してコネクション確立要求があった場合に、前記未結合ファイアウォールーサーバ間コネクションの数と前記未結合クライエントーファイアウォール間コネクションの数を比較し、サーバ側コネクション数よりクライエント側コネクション数が上回っていれば、新たにクライエントーファイアウォール間コネクションを確立し、クライエント側コネクション数がサーバ側コネクション数と同数か下回るようであれば、クライエントからのコネクション確立要求を廃棄するか、あるいは、前記未結合ファイアウォールーサーバ間コネクションの数が前記未結合クライエントーファイアウォール間コネクションの数を上回るまでクライエントーファイアウォール間コネクション確立を遅延することを特徴とする。

【００２８】（８）（１）の構成において、前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記クライエントーファイアウォール間コネクションを通じて前記クライエントからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライエントーファイアウォール間コネクションを切断し、不正なしと判定された場合に、未結合のファイアウォールーサーバ間コネクションと結合し、当該メッセージを当該ファイアウォールーサーバ間コネクションを通じて前記サーバへ転送することを特徴とする。

【００２９】（９）（８）の構成において、前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記クライエントーファイアウォール間コネクションを通じて前記クライエントからの追加のメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該クライエントーファイアウォール間コネクション及び当該クライエントーファイアウォール間コネクションと結合済みのファイアウォールーサーバ間コネクションを切断し、不正なしと判定された場合に、受信した追加のメッセージを当該クライエントーファイアウォール間コネクションと結合しているファイアウォールーサーバ間コネクションを通じて前記サーバへ転送し、不正ではないが、追加のメッセージでないと判定された場合に、受信したメッセージを当該クライエントーファイアウォール間コネクションと結合しているファイアウォールーサーバ間コネクションを通じてそのままサーバへ転送することを特徴とする。

【００３０】（１０）（１）の構成において、前記第３のステップは、前記クライエントーファイアウォール間コネクションとファイアウォールーサーバ間コネクションとの結合状態で、前記ファイアウォールーサーバ間コネクションを通じて前記サーバからのメッセージを受信した場合に、このメッセージを検証して不正の有無を判定し、不正と判定された場合に、当該ファイアウォールーサーバ間コネクション及び当該ファイアウォールーサーバ間コネクションと結合済みのクライエントーファイアウォール間コネクションを切断し、不正なしと判定された場合に、当該ファイアウォールーサーバ間コネクションと結合しているクライエントーファイアウォール間コネクションを通じて前記クライエントへメッセージを転送し、不正ではないがメッセージでないと判定された場合に、当該ファイアウォールーサーバ間コネクション

と結合しているクライエント－ファイアウォール間コネクションを通じてそのまま前記クライエントへ転送することを特徴とする。

【００３１】（１１）（３）、（４）、（５）のいずれかの構成において、前記管理収容本数を、前記サーバからの制御信号により指定・変更することを特徴とする。

【００３２】（１２）（３）、（４）、（５）のいずれかの構成において、前記管理収容本数を、一つ以上のクライエントをまとめた複数のクライエントグループが存在するとき、クライエントグループごとに指定・変更することを特徴とする。

【００３３】（１３）（３）、（４）、（５）のいずれかの構成において、前記管理収容本数を、一つ以上のサーバをまとめた複数のサーバグループが存在するとき、サーバグループごとに指定・変更することを特徴とする。

【００３４】また、本発明に係るネットワークサービス中継装置は、以下のような特徴的構成を備える。

【００３５】（１４）サーバ・クライエントサービスが行われるネットワークシステムに適用され、サーバコンピュータとクライエントコンピュータとの間で伝送される情報を中継し、ファイアウォールとして機能するネットワークサービス中継装置であって、前記サーバコンピュータとの間で予め決められた本数で、クライエント－ファイアウォール間コネクションと未結合のファイアウォール－サーバ間コネクションを確立し管理する未結合コネクション管理手段と、前記クライエントコンピュータのうち新規にコネクション要求のあったクライエントコンピュータとの間でクライエント－ファイアウォール間コネクションを確立する新規コネクション処理手段と、前記新規コネクション処理手段で確立されたクライエント－ファイアウォール間コネクションにより結合されたクライエントコンピュータからのサービス要求について正当性を検証するサービス要求正当性検証手段と、前記サービス要求正当性検証手段で正当性が認められたとき、前記クライエント－ファイアウォール間コネクションとファイアウォール－サーバ間コネクションとを結合して被検証サービス要求をサーバコンピュータに転送し、正当性が認められないとき、前記クライエント－ファイアウォール間コネクションとファイアウォール－サーバ間コネクションとの結合を切断するコネクション間中継処理手段とを具備することを特徴とする。

【００３６】（１５）（１４）の構成において、さらに、前記コネクション間中継処理手段でクライエント－ファイアウォール間コネクションとファイアウォール－サーバ間コネクションとの結合によりサーバコンピュータから送出されるサービス応答について正当性を検証するサービス応答検証手段を備え、前記コネクション中継処理手段は、前記サービス応答検証手段で正当性が認められたとき、被検証サービス要求をクライエントコンピュータに転送し、正当性が認められないとき、前記クライエント－ファイアウォール間コネクションとファイアウォール－サーバ間コネクションとの結合を切断することを特徴とする。

【００３７】（１６）（１４）の構成において、前記未結合コネクション管理手段は、ファイアウォール－サーバ間コネクションの最大収容本数が指定されているとき、クライエント－ファイアウォール間コネクションと未結合のファイアウォール－サーバ間コネクション数を最大収容本数以内に制限することを特徴とする。

【００３８】（１７）（１４）の構成において、前記ネットワークシステムがＴＣＰ／ＩＰ（Transport Communication Protocol／Internet Protocol）で構築されているとき、前記コネクション間中継処理手段は、ＴＣＰ層とＩＰ層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はＴＣＰ層に配置され、前記サービス要求正当性検証手段はアプリケーション層に配置されることを特徴とする。

【００３９】（１８）（１４）の構成において、前記ネットワークシステムがＴＣＰ／ＩＰ（Transport Communication Protocol／Internet Protocol）で構築されているとき、前記コネクション間中継処理手段は、ＴＣＰ層とＩＰ層との間に配置され、前記未結合コネクション管理手段及び新規コネクション処理手段はＴＣＰ層に配置され、前記サービス要求正当性検証手段及びサービス応答正当性検証手段はアプリケーション層に配置されることを特徴とする。

【００４０】本発明は、以上の構成によって、サービス要求の正当性を判断した上でサービス中継を高速に行うことができ、クライエントとのコネクションの確立にかかる負担を軽減し、クライエントとサーバとのコネクションの数を管理できるファイアウォールを実現する技術を提供する。

【００４１】

【発明の実施の形態】以下、図１乃至図５を参照して本発明の実施の形態を詳細に説明する。

【００４２】図１は、本発明が適用されるＴＣＰネットワークシステムの構成を示す概念図である。図１において、１１はネットワークＮ１に接続され、サーバ（Ｓ）として機能するサーバコンピュータ、１２はネットワークＮ２に接続され、クライエント（Ｃ）として機能するクライエントコンピュータであり、ネットワークＮ１とネットワークＮ２を接続する経路には、ファイアウォール（Ｆ）として機能する結合・中継モジュール１３が介在される。

【００４３】以下、上記システムに本発明を適用した場合の第１乃至第３の実施形態を説明する。

【００４４】（第１の実施形態）第１の実施形態として、本発明に係るサービス中継方法をシーケンス処理によって実現する場合について、図２に示すシーケンス図

を参照して説明する。

【００４５】図２において、まずファイアウォール（Ｆ）は、予めサーバ（Ｓ）との間でＳＹＮパケット（Ｐ１１）、ＳＹＮ／ＡＣＫパケット（Ｐ１２）、ＡＣＫパケット（Ｐ１３）のやり取りを通じてファイアウォールーサーバ間コネクションを確立しておく。

【００４６】上記ファイアウォール（Ｆ）は、クライエント（Ｃ）からのコネクション確立要求に基づくＳＹＮパケット（Ｐ１４）を受けると、ＳＹＮ／ＡＣＫパケット（Ｐ１５）、ＡＣＫパケット（Ｐ１６）のやり取りを通じてクライエントーファイアウォール間コネクションを確立する。この際、ファイアウォール（Ｆ）が使用するＳＥＱ番号は、サーバ（Ｓ）とのファイアウォールーサーバ間コネクションの確立時に当該サーバ（Ｓ）が用いた初期ＳＥＱ番号「ＳＳ」を使用する。

【００４７】その後、ファイアウォール（Ｆ）は、クライエント（Ｃ）からのデータパケット（Ｐ１７）を受け取ると、そのＳＥＱ番号「ＣＳ＋１」を、ファイアウォール（Ｆ）が確立したファイアウォールーサーバ間コネクションの初期ＳＥＱ番号「ＦＷ」に基づいてＳＥＱ番号「ＦＷ＋１」に書き換え、そのデータパケット（Ｐ１８）をサーバ（Ｓ）へ中継転送する。続いて、サーバ（Ｓ）からのＡＣＫパケット（Ｐ１９）のＡＣＫ番号「ＦＷ＋１０１」をクライエントの初期ＳＥＱ番号に基づいたＡＣＫ番号「ＣＳ＋１０１」へ書き換え、そのデータパケット（Ｐ２０）をクライエント（Ｃ）へ中継転送することにより実現する。

【００４８】上記処理におけるファイアウォール（Ｆ）での処理を図３に示す。

【００４９】まず、ファイアウォール（Ｆ）は、初期設定として、サーバ（Ｓ）との間に新しいファイアウォールーサーバ間コネクションを確立しておき、ファイアウォール（Ｆ）側とサーバ（Ｓ）側の初期ＳＥＱ番号「ＦＷ」、「ＳＳ」を保持し（Ｓ１）、次にクライエント（Ｃ）から接続要求が来るまで待機する（Ｓ２）。クライエント（Ｃ）から接続要求があれば、保持しておいたサーバ側初期ＳＥＱ番号「ＳＳ」をクライエント（Ｃ）とのコネクション確立に用いてクライエントーファイアウォール間コネクションを確立し、クライエント側初期ＳＥＱ番号「ＣＳ」を保持し（Ｓ３）、一定期間、クライエント（Ｃ）からのＴＣＰデータパケット到着を待機する（Ｓ４）。

【００５０】一定期間内にクライエント（Ｃ）からＴＣＰデータパケットが到着した場合、そのＴＣＰデータパケットはクライエントーファイアウォール間コネクションのクライエント側初期ＳＥＱ番号「ＣＳ」を元にした「ＣＳ＋△ＣＳ」をＳＥＱ番号としているので、これをファイアウォールーサーバ間コネクションのファイアウォール側初期ＳＥＱ番号「ＦＷ」を元としたＳＥＱ番号「ＦＷ＋△ＣＳ」に書き換えてからサーバ（Ｓ）へＴＣＰデータパケットを転送する（Ｓ５）。転送後、ステップＳ４に戻る。

【００５１】ステップＳ４において、一定期間内にクライエント（Ｃ）からＴＣＰデータパケットが到着しなかった場合、さらに一定期間、サーバ（Ｓ）からのＴＣＰデータパケット到着を待機する（Ｓ６）。一定期間内にサーバ（Ｓ）からＴＣＰデータパケットが到着した場合、そのＴＣＰデータパケットはファイアウォールーサーバ間コネクションのファイアウォール側初期ＳＥＱ番号「ＦＷ」を元とした「ＦＷ＋△ＦＷ」をＡＣＫ番号としているので、これをクライエントーファイアウォール間コネクションのクライエント側ＳＥＱ番号「ＣＳ」を元とした「ＣＳ＋△ＣＳ」に書き換えてからクライエント（Ｃ）へＴＣＰデータパケットを転送する（Ｓ７）。転送後、ステップＳ４に戻る。

【００５２】ステップＳ６において、一定期間内にサーバ（Ｓ）からＴＣＰデータパケットが到着しなかった場合、タイムアウトか接続先コンピュータからの要求で、ファイアウォールーサーバ間コネクション、クライエントーファイアウォール間コネクションのいずれかが切断されたか判断する（Ｓ８）。切断されていなければステップＳ４に戻る。切断されている場合には、他方のコネクションを切断して、保持しておいた各初期ＳＥＱ番号「ＦＷ」、「ＳＳ」、「ＣＳ」をクリアし（Ｓ９）、ステップＳ１に戻る。

【００５３】上記処理の結果、ファイアウォール（Ｆ）において、予めサーバ（Ｓ）との接続を確保しておくことで、クライエント（Ｃ）からの接続時のサーバ（Ｓ）への負荷軽減と、サーバ（Ｓ）とクライエント（Ｃ）との間のＴＣＰデータパケット中継時におけるＳＥＱ番号およびＡＣＫ番号の書き換えのみによる中継処理の高速化を実現することができる。

【００５４】（第２の実施形態）第２の実施形態として、本発明に係るサービス中継方法を図１に示した結合・中継モジュール１３に適用した場合について、図４に示す概念図を参照して説明する。

【００５５】図４に示す結合・中継モジュール１３は、サーバコンピュータ１１とのファイアウォールーサーバ間コネクションの最大収容本数Ｍのうち、クライエントーファイアウォール間コネクションと結合していないファイアウォールーサーバ間コネクション数をＮ本に設定し管理する未結合コネクション管理部１３１、ファイアウォールーサーバ間コネクションとクライエントーファイアウォール間コネクションとの間で中継を行うコネクション間中継処理部１３２、クライエントコンピュータ１２からの新規コネクション確立要求を処理する新規コネクション処理部１３３、新規コネクション確立時あるいは中継時におけるサービス要求の正当性を検証するサービス要求正当性検証部１３４、中継時のサービス応答の正当性を検証するサービス応答正当性検証部１３５か

ら構成される。

【００５６】上記構成において、以下に処理の流れに沿って、その動作を説明する。

【００５７】ファイアウォールを構築する結合・中継モジュール１３において、未結合コネクション管理部１３１は、サーバコンピュータ１１との間で予めＮ本のファイアウォールーサーバ間コネクションを確立しておき、そのコネクションキーを保持しておく。新規クライエントコンピュータ１２ｉから接続要求があったときに、未結合コネクション数が１以上であれば、新規コネクション処理部１３３は、未結合コネクション管理部１３１に保持されているコネクションキーを用いて、クライエントーファイアウォール間コネクションを確立させる。

【００５８】次に、サービス要求正当性検証部１３４は、結合済みクライエントコンピュータ１２１～１２ｎからのサービス要求を受けると、その正当性を検証する。また、サービス応答正当計検証部１３５は、サーバコンピュータ１１からのサービス応答を受けると、その正当性を検証する。コネクション間中継処理部１３２は、サービス要求正当性検証部１３４、サービス応答正当性検証部１３５の各検証結果が正当であったときのみ、サーバコンピュータ１１と結合済みクライエントコンピュータ１２１～１２ｎとの間の中継を行う。

【００５９】すなわち、コネクション間中継処理部１３２が中継するサービス要求は、サービス要求正当性検証部１３４が検証し、正当でなければコネクション間中継処理部１３２がクライエントコンピュータ側とサーバコンピュータ側のコネクションを切断し、そうでなければ中継を行う。同様にコネクション間中継処理部１３２が中継するサービス応答は、サービス応答正当性検証部１３５が検証し、正当でなければコネクション間中継処理部１３２がクライエントコンピュータ側とサーバコンピュータ側のコネクションを切断し、そうでなければ中継を行う。

【００６０】上記のモジュール構成によれば、結果として、サーバコンピュータ１１のコネクション数をＭ本以下に限定することができ、サーバコンピュータにかかる負荷を限定できる。また、サーバコンピュータとクライエントコンピュータ間のサービス要求及びサービス応答の正当性を検証できる。

【００６１】（第３の実施形態）第３の実施形態として、図１に示すシステムがＴＣＰ／ＩＰで構築されている場合に、本発明に係るサービス中継方法を結合・中継モジュール１３のＴＣＰ／ＩＰ階層にて実現する場合について、図５に示すＴＣＰ／ＩＰ階層構造図を参照して説明する。尚、図５において、図４と同一機能を果たすブロックには同一符号を付して示す。

【００６２】図５に示す階層構造では、ネットワークインタフェース層、ＩＰ層、ＴＣＰ層、アプリケーション層を備え、ＩＰ層とＴＣＰ層との間にコネクション間中継処理部１３２を配置し、ＴＣＰ層に新規コネクション処理部１３１、未結合コネクション管理部１３３を配置し、アプリケーション層にサービス要求正当性検証部１３４、サービス応答正当性検証部１３５を配置している。

【００６３】未結合コネクション管理部１３１は、予めサーバコンピュータ１１との間でサーバーファイアウォール間コネクションを確立し、コネクションキーを保持しておく。クライエントコンピュータ１２から新規コネクション確立要求があれば、まず、新規コネクション処理部１３３が未結合コネクション管理部１３１に保持されているコネクションキーを用いてコネクションの確立を行う。

【００６４】次に、サービス要求正当性検証部１３４がサービス要求を検証し、正当であれば、コネクション間中継処理部１３２がサービス要求をサーバコンピュータ１１に転送する。また、サービス応答正当性検証部１３５がサービス要求を検証し、正当であれば、コネクション間中継処理部１３２がサービス応答をクライエントコンピュータ１２に転送する。以後の処理は、コネクション間中継処理部１３２によるパケットヘッダの書き換えだけで中継が行われる。

【００６５】上記のＴＣＰ／ＩＰ階層でのモジュール構成によれば、結果として、「アプリケーション・ゲートウェイ」と同等のサービス要求の検証ができ、同時に以後の中継をパケットヘッダの書き換えだけにより行うため、「パケット・フィルタリング」と同等の応答速度を得ることができる。

【００６６】尚、上記の各実施形態では、サーバコンピュータとは別にファイアウォールとして機能する結合・中継モジュールを備えるシステムに適用する場合について説明したが、サーバコンピュータ自体に各実施形態の結合・中継モジュールを組み込むことも可能である。

【００６７】

【発明の効果】以上のように本発明によれば、「アプリケーション・ゲートウェイ」と同様にサービス要求の正当性まで判断する能力と「パケット・フィルタリング」と同等の応答時間の短さを兼ね備えるファイアウォールを構築したネットワークサービス中継方法及び中継装置を提供することができる。

【００６８】また、上記ネットワークサービス中継方法及び中継装置において、ファイアウォールがサーバの代わりにクライエントとの間にコネクションを確立することができ、これによって新規コネクション確立にかかるサーバの負担を軽減することができる。

【００６９】また、上記ネットワークサービス中継方法において、ファイアウォールがサーバとクライエントとの間のコネクションの数を管理することができ、これによってサービス提供にかかるサーバの負荷を管理することができる。

17

【００７０】結果として、「アプリケーション・ゲートウェイ」方式と同等の強固なサービス要求検証能力を持ちつつ、コネクション確立後は簡単な処理での中継が可能で、コネクション確立時のサーバへの負担が軽減し、クライエントとサーバの間のコネクション数を管理することのできるネットワークサービス中継方法及び中継装置を提供することができる。

【図面の簡単な説明】

【図１】　本発明が適用されるＴＣＰネットワークシステムの構成を示す概念図。

【図２】　第１の実施形態として、本発明に係るサービス中継方法をシーケンス処理によって実現する場合を説明するためのシーケンス図。

【図３】　第１の実施形態のファイアウォール（Ｆ）での処理を示すフローチャート。

【図４】　第２の実施形態として、本発明に係るサービス中継方法を結合・中継モジュールに適用した場合を説明するための概念図。

【図５】　第３の実施形態として、本発明に係るサービス中継方法をＴＣＰ／ＩＰネットワークシステムにおける結合・中継モジュール１３のＴＣＰ／ＩＰ階層にて実現する場合を説明するためのＴＣＰ／ＩＰ階層構造図。

【図６】　ＴＣＰのコネクション確立の様子を示すシーケンス図。

【符号の説明】

Ｓ…サーバ

Ｃ…クライエント

Ｆ…ファイアウォール

１１…サーバコンピュータ

１２…クライエントコンピュータ

１３…機能する結合・中継モジュール（ファイアウォール）

１３１…未結合コネクション管理部

１３２…コネクション間中継処理部

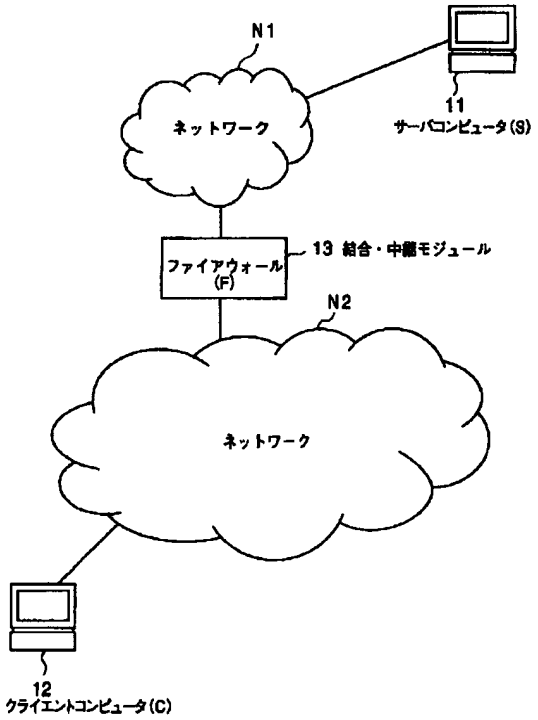
１３３…新規コネクション処理部

１３４…サービス要求正当性検証部

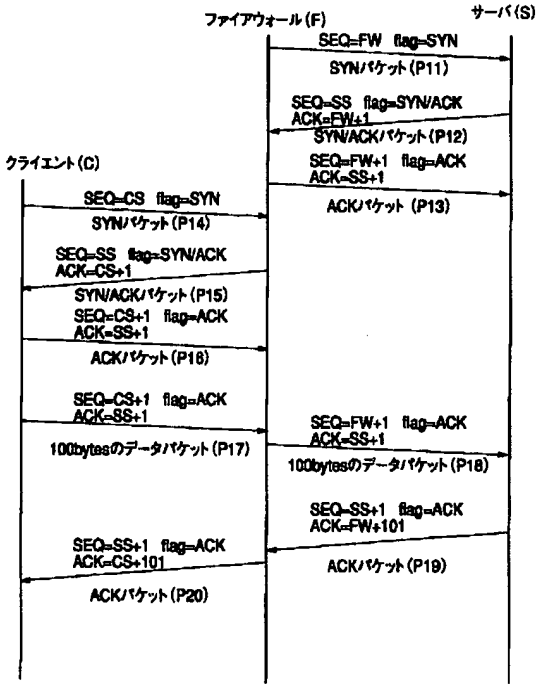
１３５…サービス応答正当性検証部

18

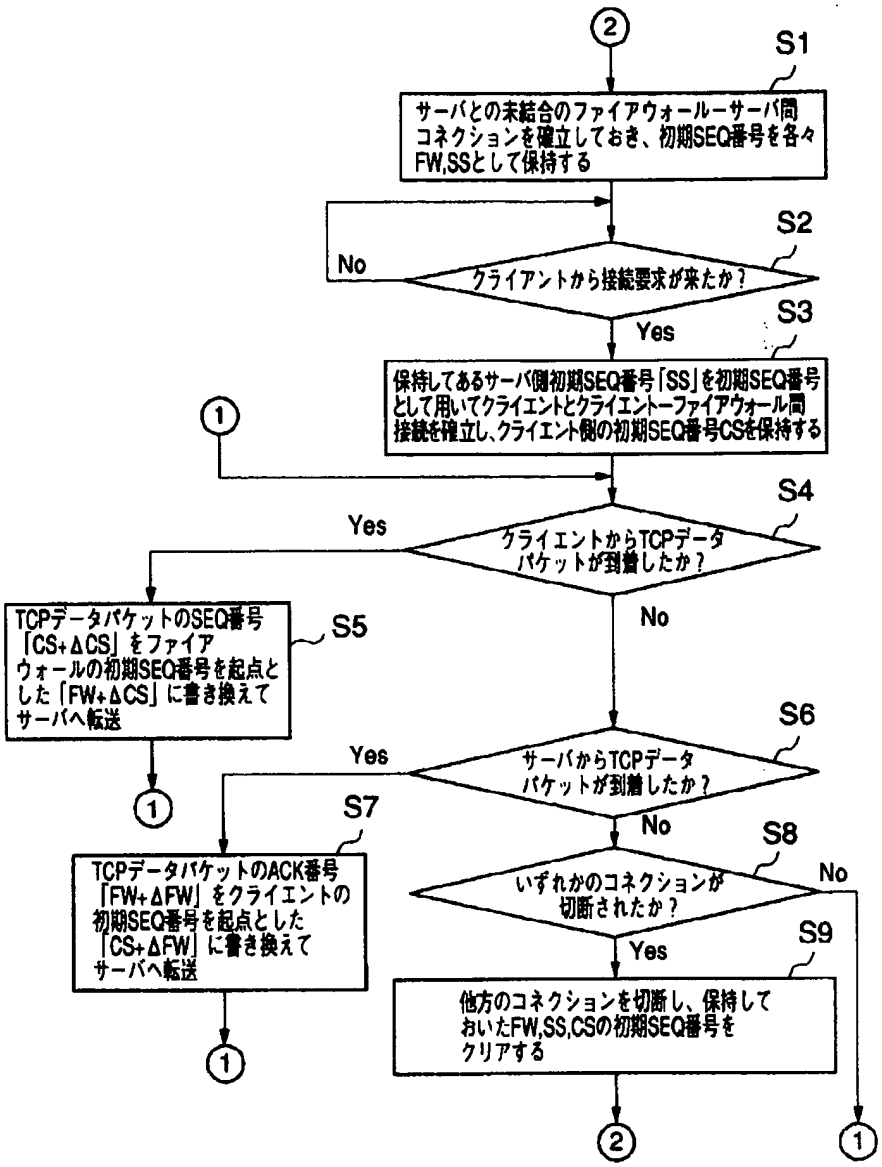
【図１】



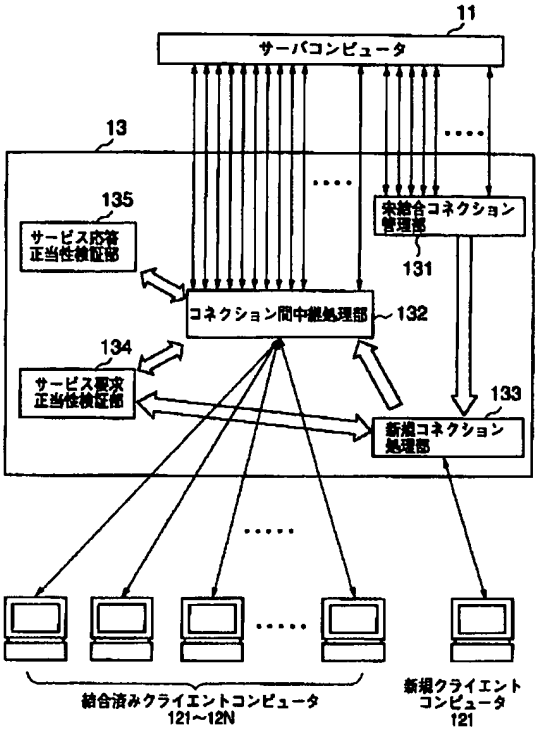
【図２】



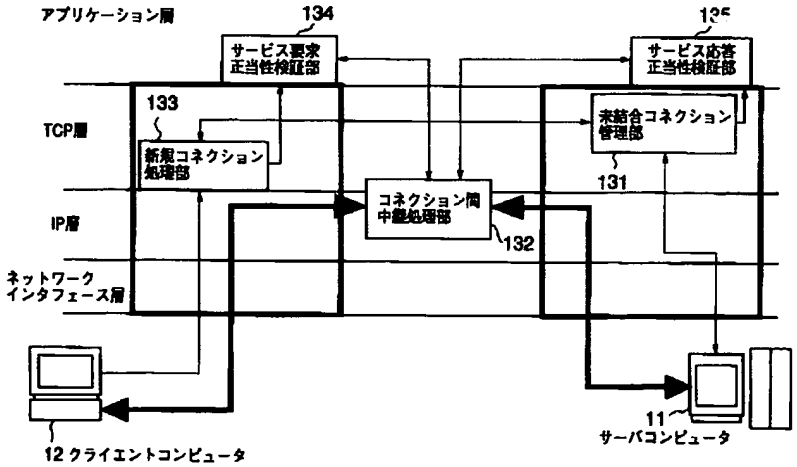
【図３】


②
S1
サーバとの未結合のファイアウォールーサーバ間コネクションを確立しておき、初期SEQ番号を各々FW,SSとして保持する
S2
No
クライアントから接続要求が来たか？
Yes
S3
保持してあるサーバ側初期SEQ番号「SS」を初期SEQ番号として用いてクライエントとクライエントーファイアウォール間接続を確立し、クライエント側の初期SEQ番号CSを保持する
①
S4
Yes
クライエントからTCPデータパケットが到着したか？
No
TCPデータパケットのSEQ番号「CS+ΔCS」をファイアウォールの初期SEQ番号を起点とした「FW+ΔCS」に書き換えてサーバへ転送
S5
①
S6
Yes
サーバからTCPデータパケットが到着したか？
No
S7
TCPデータパケットのACK番号「FW+ΔFW」をクライエントの初期SEQ番号を起点とした「CS+ΔFW」に書き換えてサーバへ転送
①
S8
No
いずれかのコネクションが切断されたか？
Yes
S9
他方のコネクションを切断し、保持しておいたFW,SS,CSの初期SEQ番号をクリアする
②
①

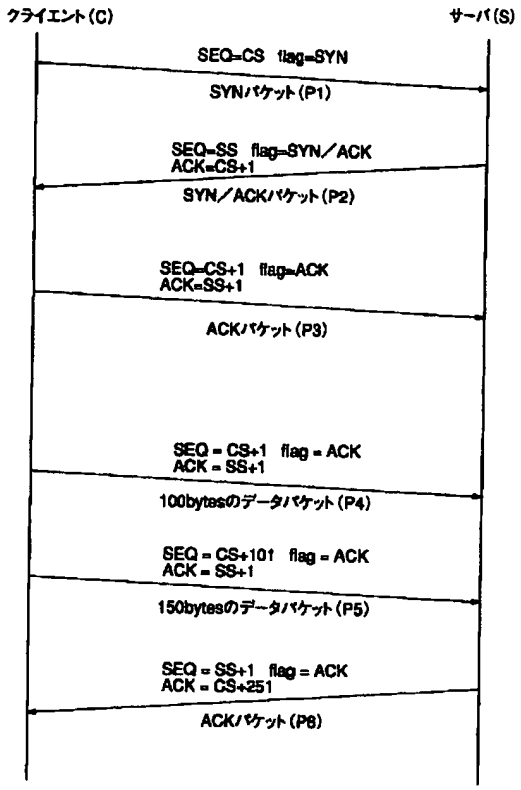
【図４】


11
サーバコンピュータ
13
135
サービス応答
正当性検証部
未結合コネクション
管理部
131
コネクション間中継処理部
132
134
サービス要求
正当性検証部
133
新規コネクション
処理部
結合済みクライエントコンピュータ
121～12N
新規クライエント
コンピュータ
121

【図５】


アプリケーション層
134
サービス要求
正当性検証部
サービス応答
正当性検証部
133
TCP層
新規コネクション
処理部
未結合コネクション
管理部
131
IP層
コネクション間
中継処理部
132
ネットワーク
インタフェース層
12 クライエントコンピュータ
11
サーバコンピュータ

【図６】



フロントページの続き

(72)発明者　盛合　敏
東京都千代田区大手町二丁目３番１号　日
本電信電話株式会社内

Ｆターム(参考)　5B089 GA04 GB01 HB18 KA05 KA17
KB13 KG03 KG07
5K030 GA02 GA15 HA08 HD03 JA11
JT06 LB01 LB19